Security

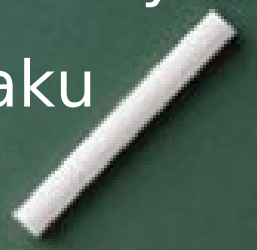
narzędzie oszczędności

Jakub Tomaszewski

Jakub Masłowski

Statystyki

- **45%** firm instaluje regularnie patche
- **60%** awarii spowodowanych nie autoryzowanymi zmianami
- **37%** zamierza wydać więcej $ niż w roku poprzednim
- **56%** zamierza wprowadzić monitoring (ruch/bazy danych)
- **41%** uważa za uzasadnione wydatki na security
- **73%** małych i średnich firm było celem ataku



- **29% uważa za realne zagrożenia cyber ataków**

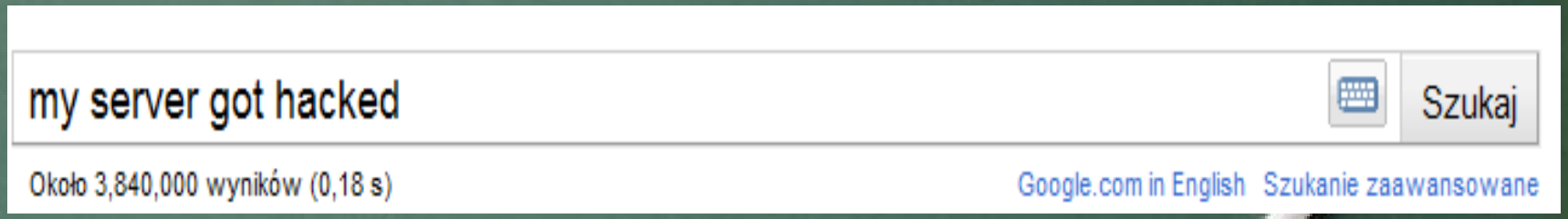
Jak przekonać „biznes” do „security”

Ready for disaster number two? According to Japan's Nikkei news service, the second breach involved the theft of *12,700 credit card numbers*.

Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?

June 10, 2010, 9:45AM

Mass SQL Injection Attack Hits Sites Running IIS



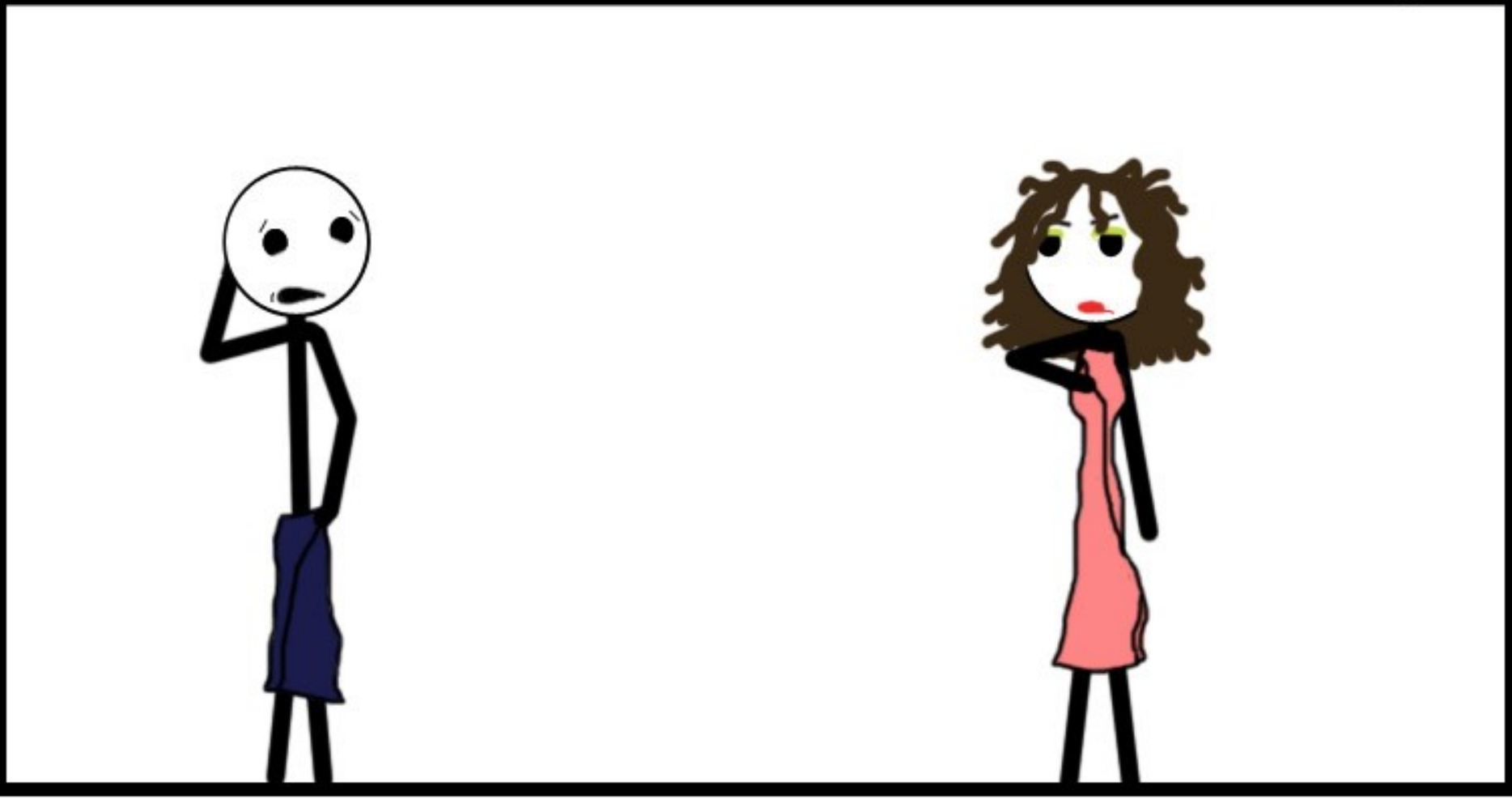
Missing BP laptop had spill victim claim data

Lost computer held thousands of Social Security numbers, all unencrypted

Jak najtaniej się uczyć?

… na błędach innych!

"Lesson Learned #9"



Always ask before going anal.

Pro aktywny proces utrzymania bezpieczeństwa IT

- Regularne audyty,
- Stała identyfikacja zagrożeń,
- Profilowanie ryzyka,
- Rozpatrywanie kontekstowe,
- Świerze spojrzenie.

Better late than never?

Anti-DDoS specialists, Prolexic Technologies were brought on by Sony to stop the mass attack of the site's servers:

> *Prolexic has been fighting DDoS attacks and developing "best of breed" practices and a massive global network for over 7 years. Our experience is simply unmatched.*
>
> *Prolexic's services provide online businesses with the most advanced protection available against DDoS attacks and malicious botnet activity.*

Speaking on the Anonymous IRC, several members expressed their frustration at the new defenses, which have (mostly) managed to stop the sites being taken down:

> *prolexic is holding up*
>
> *…i doubt we can ddos prolexic*
>
> *…you wont kill prolexic with l**c*
>
> *…it's getting harder to ddos store.ps.com*

Automatyzowanie procesów

- Automatyczne wymuszenia zmiany hasła,
- Skrypty do weryfikacji konfiguracji,
- Nadzór nad zmianami,
- Aktywny monitoring,
- Dowolna inna redukcja "human error"

According to the survey, 66 percent of respondents cited human error in the configuration of network devices as the most common cause of outages in the past 12 months, followed by capacity overload (14 percent) and flaws in the gateway product (9 percent). The majority of respondents claimed to have anywhere from ten to forty-nine different security gateways installed on their network. Another 15 percent of companies had more than fifty security gateways installed.

Monitorowanie aktywności

System = żywy organizm

Problemy:

- zmiany,
- poprawki,
- błędy,
- modyfikacja danych.

The news comes less than a week after Sony alerted customers that a hacker broke into Sony's PlayStation video game network and stole names, addresses, passwords and possibly credit card numbers of its 77 million customers.

"In the course of our investigation into the intrusion into our systems we have discovered an issue that warrants enough concern for us to take the service down effective immediately," the company said on its web site.

Sony waited almost a week before they released a statement regarding the hacking of its network. Sony's PlayStation 3 has almost 80 million gamers. Think they deserve an explanation? Some peace of mind about the security of their private data?

Wiedza to broń

Najgroźniejszą broń → wiedza,

Największa słabość → brak wiedzy

Szkolenia bezpieczeństwa
na wszystkich poziomach!

Czy bezpieczeństwo się opłaca?

Bezpieczeństwo stacji roboczych = $$$

Support serwerów = $$$

Urządzenia bezpieczeństwa = $$$

Szkolenia = $$$

Audyty = $$$

Czyli ... ?

GoDaddy Hacks Due To Old Software – Bad Passwords

Detecting Outdated Software

An unofficial report, specifically a Pastebin link with a chat log, was published and disclosed that Sony was running outdated Linux software (Sony has since denied these claims):

- Apache 2.2.15
- Linux kernel 2.6.9-2.6.24

Bezpieczeństwo vs. VIP

Wysokie stanowiska,

Dostęp do krytycznych danych,

Wykorzystywanie stanowisk dla wygody,

Brak świadomości.


VIP

Ewidencja

Naklejka na każdym monitorze, zasilaczu, laptopie nie jest niczym nadzwyczajnym,

Ewidencja oprogramowania, też jest coraz bardziej popularna,

Więc dlaczego ewidencja miejsc i sposobu przetrzymywania kluczowych danych aż tak dziwi !?

TOKYO (Reuters) - Sony said on Saturday it had removed off the Internet the personal details of 2,500 people that had been stolen by hackers and posted on a website.

The data included names and some addresses, which were in a database created in 2001, a Sony spokeswoman said.

Zmienność

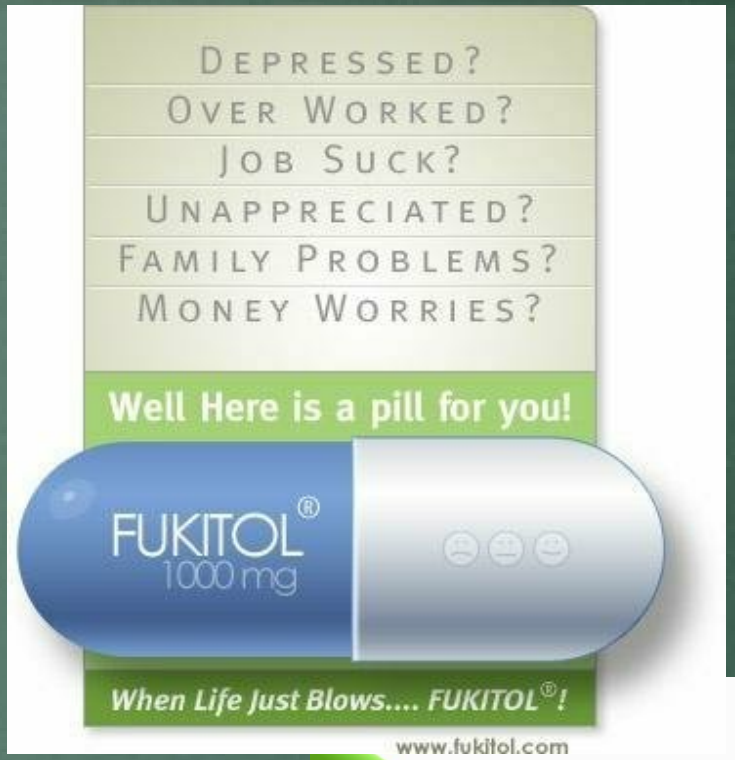
Ta cecha to nie tylko domena kobiet ;)

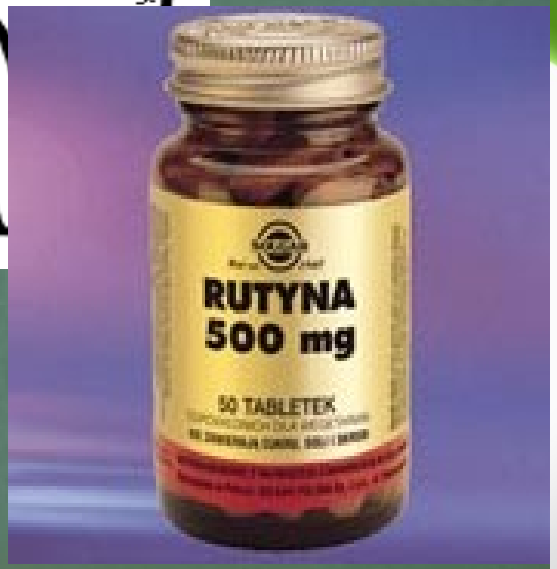
Security to także zmiany!

Rutyna wprowadza błędy

Zmieniaj i zaskakuj a mniejsza szansa,
że sam zostaniesz zaskoczony.


CHCIAŁAM ZMIENIĆ ZDANIE, ALE ZMIENIŁAM ZDANIE


DEPRESSED?
OVER WORKED?
JOB SUCK?
UNAPPRECIATED?
FAMILY PROBLEMS?
MONEY WORRIES?
Well Here is a pill for you!
FUKITOL®
1000 mg
When Life Just Blows.... FUKITOL®!
www.fukitol.com


RUTYNA
500 mg
50 TABLETEK

Odpowiedzialność

Role I obowiązki – podstawą rozliczalności

Jasno zdefiniowane obowiązki i obszary pomogą dbać o zachowanie najwyższych standardów.

RESPONSIBILITY

oops

Komunikacja

Polityki,

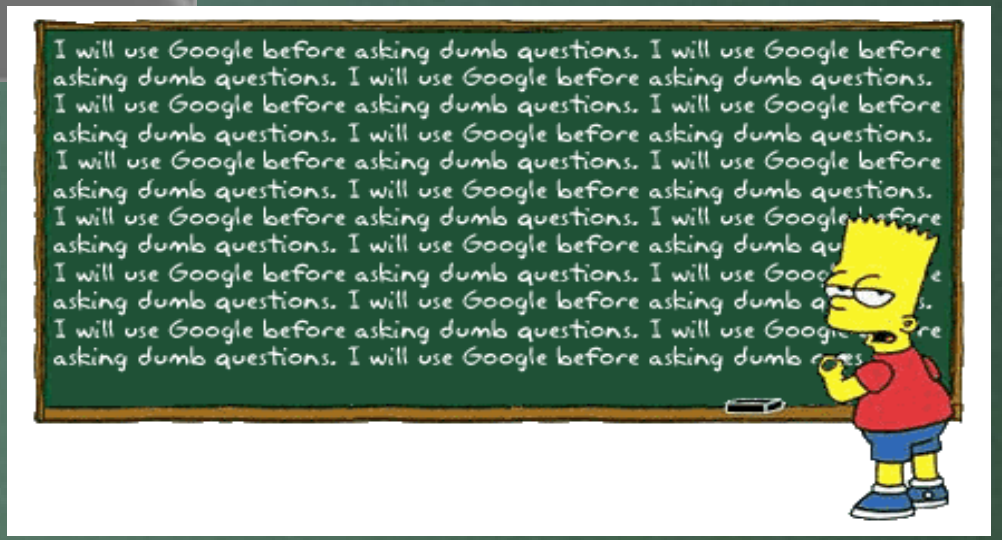
Procedury,

Instrukcje

FAQ,

How-To,

Wiki.


I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions.

Ilu pracowników wie gdzie wyszukać polityki bezpieczeństwa w Waszej firmie?

Kontakt

Kuba Masłowski
kuba.maslowski@gmail.com

Jakub Tomaszewski
bluerose.pl@gmail.com